MARCH 2022

# A HOLISTIC APPROACH TO SECURITY IN MPS

*Nicola De Blasi, CEO MPS Monitor*

MPS Monitor
Printer Monitoring in the Cloud

# A Holistic Approach to Security in MPS

Although COVID-19 has had a major impact on the office technology industry, in the long run, poor security is more likely to damage your MPS business than COVID-19. The low print volumes and accelerated digital transformation trends caused by the pandemic aren't necessarily good for MPS providers, but eventually we can expect workers to go back into the office, page volumes to return to healthy levels, and MPS providers to carry on.

Compare that to a security breach. Not only does that create a significant financial impact, but there is also an impact on your reputation. Finding new customers and holding on to the ones you've worked hard to get is difficult enough — try doing it as "that MPS provider who got hacked." If you sell MPS, then security needs to be a top priority.

## Infrastructure

Ironically, the very remote monitoring and management technology that MPS providers rely on to run their businesses efficiently can also be the source of increased cybersecurity risks. The data collection agent (DCA) enables MPS dealers to remotely collect vital information about fleet status, meters, consumables, and so on. Most modern DCAs are self-updating, constantly exchanging data with cloud services. What if someone pulls off a man-in-the-middle attack or pushes down a malicious code through a supply-chain intrusion? Suddenly, the DCA transforms itself from a useful and benign tool into a silent and effective C2 (Command and Control) attack vector for cybercriminals.

Cloud providers should be performing routine penetration testing and vulnerability assessments and have continuous security monitoring procedures in place. A comprehensive cybersecurity approach involves compliance to broadly recognized security standards, like ISO/IEC 27001 and AICPA SOC 2 Trusted Services Criteria. The combination of standards compliance with adequate tools and procedures can ensure that an Information Security Management System (ISMS) is developed and maintained using a methodology that assesses and mitigates cybersecurity risks and undergoes a continuous improvement process to prevent, or at least mitigate, attacks.

## Data security and compliance

MPS providers are responsible for handling a lot of sensitive business information, personally identifiable information (PII), technical information regarding their customers' IT infrastructure, and other valuable data. When processing data protected by regulations, it is incumbent upon the MPS provider to ensure it stays compliant. Laws governing compliance are increasingly common in the U.S. as well as Europe, and navigating the privacy landscape can be tricky, so it's essential to work with a provider that stays up to date on compliance. Learn more about various privacy laws and regulations here.

## Device security

Printers are some of the most neglected devices in a customer's network when it comes to IT security. An MPS provider should not only be concerned about keeping print volumes controlled and consumables refreshed – they should make sure each contracted device is managed from a security perspective as well. Many businesses don't have any formal security policies, which leads to devices with bad configurations or outdated firmware with known vulnerabilities.

The scale of the risk this poses, can be seen in Quocirca's recent Cloud Print Services 2021 report. It found that only 21% of those organisations surveyed are completely confident in the security of their print environment since the onset of the pandemic, compared to 33% pre-pandemic. Additionally, 32% indicated that employee-owned printers present a risk to their organisation, which must do more to protect cloud data from phishing attacks, malware, ransomware and a host of other vulnerabilities.

Cybercriminals are aware of this and often target printers and MFPs for that reason. MPS providers must work with customers to make sure devices are secure, enact smart security policies, and make sure that those policies are always in effect. Some solutions can automate that process, checking devices against a security policy and remediating non-compliant devices to the proper configuration.

## User security

Users are the main cause of security breaches, and while you cannot prevent every incident, MPS providers can save users from themselves. User accounts should be locked down and built on the principles of "need to know/need to use."

The best security option is to integrate an MPS provider's cloud applications into Active Directory (AD) and enable SaaS Single Sign-On, ensuring users don't need different (possibly weak) credentials for each system and allowing users to be granted the minimum privileges needed.

When AD integration is not possible, simple fixes, like enforcing strong passwords, requiring users to change their password every six months (or sooner), and implementing Two-Factor Authentication (2FA) can prevent cybercriminals from taking control of an employee's accounts. There are some more sophisticated steps that you can take as well, like creating user profiles with granular permissions settings based on the user's job function or automatically masking confidential data and PII when displayed.

## Cloud print in the work-from-home environment

The shift to home offices poses new, additional challenges for IT decision makers, and more businesses will need to move their print servers to the cloud to allow their employees to print in a secure and managed way. Quocirca's report suggests that "The hybrid workplace is here to stay, and it is imperative that organizations mitigate the risk of data loss by protecting printing endpoints in both the home and office environments."

In July 2020, when Microsoft first announced the public preview of its cloud-based Universal Print, IDC noted: "Businesses of all sizes are showing increased interest in cloud-based print and print management … the COVID-19 pandemic has had a dramatic impact on how work gets done, leading to more remote employees and the need to create stable and secure work-from-home environments."

Referring specifically to how this impacts print, Quocirca's 2021 MPS study reported that 39% of organisations have implemented some form of cloud print management platform, rising to 48% in organisations with more than 1,000 employees, 52% in the US and 51% in the financial services sector. To support the needs of remote workers printing to printers located in the office, 47% indicated that they have implemented remote job submission to office devices, rising to 58% in the US and 53% in the financial sector.

Overall, 67% said that they will increase their use of cloud print management by 2025, with a further 5% saying that they will move over to cloud-based printing completely. Notably, those using a hybrid MPS, rather than a fully outsourced MPS, are more likely to transition to cloud-based printing (80% and 63% respectively).

## IT security remains the top investment priority over the next 12 months

The recent Quocirca's Global Print Security Landscape 2022 report reveals that many organisations are struggling to keep up with print security demands in today's hybrid work environment.
53% of respondents say IT security is one of their highest three priorities. MPS (managed print services) are second in importance (41%) followed by managed IT services (38%) and cloud services (35%). 70% of organisations expect to increase their print security spend over the next 12 months, with only 11% expecting a decrease

## Moving forward

Cloud print and remote management technologies are powerful tools that help MPS providers deliver top-notch service at lower prices. But they also introduce new risks to the MPS model, such as a much larger attack surface and more privacy regulations that must be followed. And while adequate security and regulatory compliance are no easy feats, they are not impossible either.

The tools and partners already exist. One such example according to Keypoint Intelligence, is MPS Monitor 2.0. In Keypoint Intelligence's Managed Print Services Platform Security Whitepaper, it declared that MPS Monitor's solution had met key criteria, ranging from the ability to maintain customer devices in a stringent security posture through proactive and automated management of key device settings, to offering a proven-secure DCA for their customers' networks. The Whitepaper declared that MPS Monitor also offers a proven-secure back-end system that protects customer data, as well as a proven-secure cloud infrastructure that undergoes continuous security testing and auditing from specialised security teams. The Whitepaper also noted that its full and comprehensive set of policies and procedures meets the requirements for industry-standard security certifications.

Clearly, it's just a matter of doing your homework: choosing the right technologies, ensuring compliance with standards, and keeping yourself committed.

*Note:*

*"This blog is an adjusted version of the one that originally appeared on The Imaging Channel"*

MPSMonitor
Printer Monitoring in the Cloud